

Matt Putterman (CA Bar No. 306845)  
**PUTTERMAN LAW, APC**  
23 Corporate Plaza Drive - Suite 150  
Newport Beach, CA 92660  
Telephone: (949) 271-6382  
E-Mail: [Matt@Putterman-Law.com](mailto:Matt@Putterman-Law.com)

David C. Silver, Esq. (*pro hac vice* forthcoming)  
**SILVER MILLER**  
11780 W. Sample Road  
Coral Springs, Florida 33065  
Telephone: (954) 516-6000  
E-Mail: [DSilver@SilverMillerLaw.com](mailto:DSilver@SilverMillerLaw.com)

*Attorneys for Plaintiff Daniel Fraser*

**UNITED STATES DISTRICT COURT**  
**FOR THE NORTHERN DISTRICT OF CALIFORNIA**

DANIEL FRASER, an individual;

Plaintiff,

v.

MINT MOBILE, LLC, a Delaware limited  
liability company;

Defendant.

Case No. \_\_\_\_\_

**COMPLAINT FOR:**

- (1) DECLARATORY JUDGMENT**
- (2) BREACH OF FEDERAL COMMUNICATIONS ACT [47 U.S.C. §§ 206, 222]**
- (3) VIOLATION OF COMPUTER FRAUD AND ABUSE ACT (“CFAA”) [18 U.S.C. § 1030(a)(2)(C) and 1030(a)(4)]**
- (4) VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW - CAL. BUS. & PROF. CODE § 17200 *et seq.***
- (5) VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW - CAL. BUS. & PROF. CODE § 17200 *et seq.***
- (6) VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW - CAL. BUS. & PROF. CODE § 17200 *et seq.***
- (7) NEGLIGENCE**
- (8) NEGLIGENT MISREPRESENTATION**
- (9) NEGLIGENT TRAINING AND SUPERVISION**
- (10) BREACH OF CONTRACT**
- (11) BREACH OF IMPLIED CONTRACT**
- (12) BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING**

1 Plaintiff DANEIL FRASER, an individual (hereafter referred to as “Plaintiff”), by and through  
 2 undersigned counsel, hereby sues Defendant MINT MOBILE, LLC, a Delaware limited liability  
 3 company (“Defendant” or “MINT”), for damages and equitable relief. As grounds therefor, Plaintiff  
 4 alleges the following:

5 **PRELIMINARY STATEMENT**

6 1. This action is brought by Plaintiff, a MINT customer who lost approximately Four  
 7 Hundred Sixty-Six Thousand Dollars (\$466,000.00) worth of cryptocurrency in an ongoing identity  
 8 theft crime called “SIM hijacking.”

9 2. A subscriber identity module, widely known as a “SIM card,” stores user data in phones  
 10 on the Global System for Mobile (GSM) network -- the radio network used by MINT, operating on T-  
 11 Mobile’s GSM-based network, to provide cellular telephone service to its subscribers.

12 3. MINT is a mobile virtual network operator (“MVNO”) that operates on the  
 13 infrastructure of T-Mobile’s existing network.

14 4. SIM cards are principally used to authenticate cellphone subscriptions; as without a SIM  
 15 card, GSM phones are not able to connect to T-Mobile’s telecommunications network.

16 5. Not only is a SIM card vital to using a phone on the MINT network, the SIM card also  
 17 holds immeasurable value as a tool to identify the user of the phone -- a power that can be corrupted to  
 18 steal the identity of that user.

19 6. Preserving the security surrounding a MINT accountholder’s SIM card and account with  
 20 the phone carrier is a duty of paramount importance.

21 7. MINT expressly acknowledges that MINT’s consumers “*have a right, and [Mint*  
 22 *Mobile] has a duty, to protect the confidentiality of information regarding your telephone use, the*  
 23 *services you purchase from us, the calls you place and the location of your device on our network when*  
 24 *you make a telephone call*” and that once MINT “*receive[s] your personal information, we take steps*  
 25 *that we believe are reasonable to limit access to your personal information to only those employees*  
 26 *and service providers whom we determine need access to the personal information to provide the*  
 27 *requested products, services, offers or opportunities that may be of interest to you or that you have*  
 28 *ordered.*”

8. Likewise, MINT acknowledges *“us[ing] technology and security features and strict policy guidelines to safeguard the privacy of CPNI and protect it from unauthorized access or improper use. Mint Mobile does not disclose CPNI outside of Mint Mobile, its affiliates and their respective agents without customer consent except as required by law.”*

9. Those statements are consistent with MINT’s duties and obligations under the Federal Communications Act of 1934 and the pertinent implementing regulations.

10. Moreover, MINT is well aware of the pervasive harm posed by SIM hijacking, as its co-founder Rizwan Kassim has publicly acknowledged the issue as far back as 2019.<sup>1</sup>

11. Notwithstanding the importance of the duty MINT concedes that it bears, MINT breached its duty to safeguard the data it had collected from and about Plaintiff; and MINT facilitated the theft of Plaintiff’s identity and his assets.

12. As reported by numerous media sources<sup>2</sup>, MINT exposed to hackers and countless unauthorized persons on or about June 8, 2021 through June 10, 2021 the personal identifying information of a number of MINT subscribers, including the subscribers’ names, addresses, e-mail addresses, phone numbers, account numbers, and passwords.

**13. Plaintiff was among the unfortunate MINT subscribers whose personal information was exposed by MINT in June 2021.**

14. Shortly after the data breach, MINT confirmed in an e-mail to Plaintiff that his MINT account had been compromised and that, as a result, his phone number has been ported to another mobile telecommunications carrier:

---

<sup>1</sup> See, e.g., “SIM hijacking/Port Out Fraud: we might be at risk!”, *Reddit* (January 7, 2019), [https://www.reddit.com/r/mintmobile/comments/adjdw7/sim\\_hijacking\\_port\\_out\\_fraud\\_we\\_might\\_be\\_at\\_risk/](https://www.reddit.com/r/mintmobile/comments/adjdw7/sim_hijacking_port_out_fraud_we_might_be_at_risk/).

<sup>2</sup> See, e.g., “Mint Mobile hit by a data breach after numbers ported, data accessed,” *Bleeping Computer* (July 10, 2021), <https://www.bleepingcomputer.com/news/security/mint-mobile-hit-by-a-data-breach-after-numbers-ported-data-accessed/>; “Hackers Access Personal and Call Information and Port Numbers in Mint Mobile Data Breach,” *CPO Magazine* (July 22, 2021), <https://www.cpomagazine.com/cyber-security/hackers-access-personal-and-call-information-and-port-numbers-in-mint-mobile-data-breach/>.

1       **From:** Mint Mobile VIP <vip@mintmobile.com>  
 2       **Date:** July 9, 2021 at 5:03:55 PM PDT  
 3       **Subject:** Important message from Mint Mobile VIP Care

4       Between June 8, 2021 and June 10, 2021, a very small number of Mint  
 5       Mobile subscribers' phone numbers, including yours, were temporarily  
 6       ported to another carrier without permission. While we immediately took  
 7       steps to reverse the process and restore your service, an unauthorized  
 8       individual potentially gained access to some of your information, which  
 9       may have included your name, address, telephone number, email  
 10      address, password, bill amount, international call detail information,  
 11      telephone number, account number, and subscription features.

12      Attached hereto as **Exhibit "A"** is a true and correct copy of the entire July 9, 2021 message sent by  
 13      MINT to Plaintiff.

14      15.     MINT ported out Plaintiff's phone number to an unauthorized person in an unauthorized  
 15      manner on June 11, 2021 even though just days earlier (June 8, 2021), Plaintiff had implemented "PIN  
 16      verification" on his MINT account which, for security purposes, required anyone contacting MINT to  
 17      provide a one-time temporary passcode to make any changes on Plaintiff's account, including  
 18      transferring his phone service to a different telecommunications provider.

19      16.     On June 11, 2021, swiftly following MINT's release of Plaintiff's personal identifying  
 20      information and account to an unauthorized person, Plaintiff was robbed of his assets -- an act that  
 21      would not have happened but for MINT providing the unauthorized person all of the tools needed to  
 22      commit such a heinous and devastating act.

23      17.     "SIM hijacking" is not merely an ongoing crime; it is a booming crime -- especially one  
 24      that targets cryptocurrency investors.

25      18.     Over the past three years alone, undersigned counsel has represented nearly three  
 26      hundred (300) SIM hijacking victims across the country whose individual cryptocurrency losses have  
 27      ranged from as little as \$3,000.00 to as much as \$12,500,000.00.

28      19.     Notwithstanding MINT's knowledge of the prevalence of SIM hijacking and its  
 assurance that it was actively protecting its customers, those measures did not adequately protect  
 Plaintiff from the harm he suffered.

20. Furthermore, in a Criminal Complaint filed by the U.S. Department of Justice in a Michigan federal court in mid-2019<sup>3</sup>, it is painfully apparent that employees at cellphone service providers are willingly responding to solicitations to join criminal enterprises focused on effectuating SIM hijacks. As stated in the Criminal Complaint, the U.S. Attorney's Office has evidence demonstrating that AT&T employees Jarratt White and Robert Jack and Verizon employee Fendley Joseph (in return for payment) **actively, knowingly, and intentionally assisted a criminal enterprise known as "The Community" by providing Personal Identifiable Information (PII) for targeted cellphone customers**; and that with the PII that the cellphone carrier employees provided, members of The Community would then call the cellphone carriers and impersonate each target customer to get the target's phone number reassigned to a device controlled by The Community. At the present time, it is believed that The Community -- with assistance from employees at numerous cellphone service providers -- facilitated SIM hijacks leading to the theft of more than \$2,200,000.00 of cryptocurrency from targeted cellphone service accountholders.

21. As a result of MINT's failures if not active participation in SIM port theft that was inflicted upon him, Plaintiff had approximately **Four Hundred Sixty-Six Thousand Dollars (\$466,000.00)** of assets stolen from him in **June 2021**.

22. Plaintiff seeks compensatory and equitable relief restoring to him the assets and funds that were illegally taken from him.

## **THE PARTIES**

### **PLAINTIFF**

23. Plaintiff DANIEL FRASER ("Plaintiff" or "FRASER") is an individual domiciled in San Ramon, California and is *sui juris*. At all times material, Plaintiff has been an accountholder and subscriber with MINT. Among other things, Plaintiff's subscription with MINT permitted Plaintiff to use his cellphone for the following -- all of which Plaintiff in fact did with his phone: make and receive telephone calls with people around the world, send and receive text messages with people around the world, and access the internet and websites around the world through one or more web browsers.

---

<sup>3</sup> *U.S.A. v. Jarratt White, Robert Jack, and Fendley Joseph*, U.S. Dist. Ct. - Eastern District of Michigan, Case No. 2:19-mj-30227.

**DEFENDANT**

24. Defendant MINT is a Delaware limited liability company which lists its principal place of business in Costa Mesa, California. MINT functions as a mobile virtual network operator (MVNO) on T-Mobile's cellular network, meaning it uses T-Mobile's network but is not owned by T-Mobile. MINT provides wireless service to subscribers in the United States and Puerto Rico.

**JURISDICTION AND VENUE**

25. This Court has original jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, because the matter in controversy arises under the laws of the United States.

26. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

27. This Court has personal jurisdiction over Defendant because: (a) Defendant is operating, present, and/or doing business within this District, and (b) Defendant's breaches and unlawful activity occurred within this District.

28. Venue is proper pursuant to 28 U.S.C. § 1391 in that Defendant resides in this judicial district and Defendant is subject to the court's personal jurisdiction with respect to this action. In light of the foregoing, this District is a proper venue in which to adjudicate this dispute.

**GENERAL FACTUAL ALLEGATIONS****MINT MOBILE'S BUSINESS AND CUSTOMER ASSURANCES**

29. MINT markets and sells wireless telephone service through wireless service plans online only.

30. In connection with its wireless services, MINT maintains wireless accounts enabling its customers to have access to information about the services they purchase from MINT.

31. It is widely recognized that mishandling of customer wireless accounts can facilitate identify theft and related consumer harms.

32. MINT expressly acknowledges that MINT customers "*have a right, and Mint Mobile has a duty, to protect the confidentiality of [your Customer Proprietary Network Information].*"

33. Among other things, MINT's Privacy Policy states: "*We take precautions and have implemented certain technical measures intended to protect against unauthorized access to, disclosure*

1 of, and unlawful interception of [your] personal information. \*\*\* Once we receive your personal  
 2 information, we take steps that we believe are reasonable to limit access to your personal  
 3 information....”

4 34. Despite these statements and other similar statements, MINT fails to provide reasonable  
 5 and appropriate security to prevent unauthorized access to customer accounts.

6 35. Under MINT’s procedures, an unauthorized person -- including MINT’s own agents and  
 7 employees acting without the customer’s permission -- can easily impersonate the identity of the  
 8 accountholder and then access and make changes to all the information that a legitimate customer could  
 9 access and to which the customer could make changes if the customer were so authorized. For example,  
 10 a simple Google search may reveal the information used to verify the identity of an accountholder, such  
 11 as an address, zip code, telephone number, and/or e-mail address.

12 36. MINT also fails to adequately disclose that its automated processes or human  
 13 performances often fall short of its express and implied representations or promises.

#### 14 HOW SIM PORTING WORKS

15 37. “SIM hijacking” is a growing crime in the telecommunications world that requires little  
 16 more than a thorough Google search, a willing and/or negligent telecommunications carrier  
 17 representative, and an electronic or in-person impersonation of the victim.

18 38. “SIM hijacking” normally takes one of two forms: “**SIM swapping**” (in which the  
 19 victim’s telephone service is transferred to an unauthorized person serviced by the same mobile  
 20 telecommunications provider as the victim) or “**SIM porting**” (in which the victim’s telephone service  
 21 is transferred to an unauthorized person serviced by a mobile telecommunications carrier different from  
 22 that of the victim). Although the path to the hijacking is slightly different between the two, the results  
 23 to the victim are the same -- loss of mobile telephone service, identity theft, and oftentimes theft of  
 24 assets.

25 39. In the instant matter, because Plaintiff is the victim of a SIM port, that is the path that  
 26 will be discussed herein.

27 40. The theft begins when MINT -- acting through MINT agents -- allows an unauthorized  
 28 person access to a wireless telephone account without the knowledge of the accountholder.

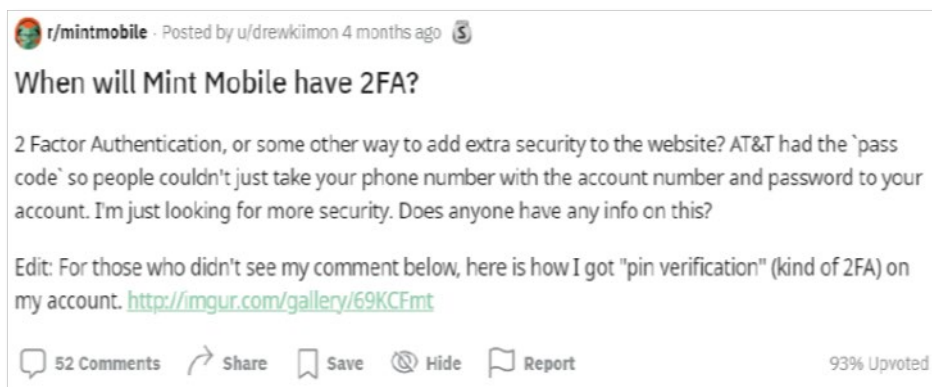
41. Often working in tandem with MINT employees -- who purposefully or negligently leak consumer data to third parties and/or the internet as a whole -- an unauthorized person using the personal identifying information provided by MINT instructs a mobile telecommunications provider like AT&T Wireless, T-Mobile, or Verizon to contact MINT's technical support department with a computerized request to transfer the victim's MINT phone service to the alternative mobile telecommunications provider under the guise that the individual making the request to transfer service is actually the victim.

42. In actuality, the unauthorized person acts intending to assume the electronic identity of the target of the crime by possessing and utilizing information that only MINT should have.

43. Under current federal regulations, the only identifying criteria required to process a request for a SIM port are: (1) 10-digit telephone number, (2) customer account number, (3) 5-digit ZIP Code of the accountholder's registered service address, and (4) passcode [if applicable].

44. Upon information and belief, MINT undertakes no measures beyond those minimal requirements to ensure the legitimacy of a SIM port request.

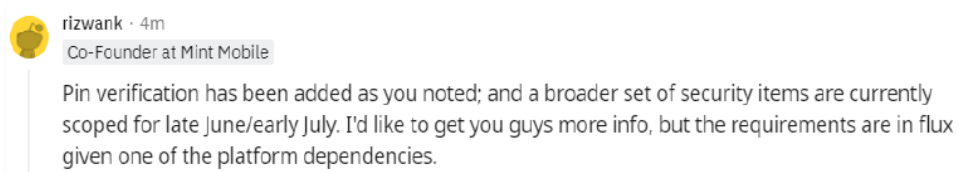
45. According to an April 2021 posting on Reddit.com<sup>4</sup>, MINT's glaring lack of security to prevent unauthorized port out requests exposed all MINT subscribers to SIM hijacking:



46. Upon further information and belief, according to MINT co-founder Rizwan Kassim's response to the above-cited criticism, MINT only recently instituted a function that would allow some

<sup>4</sup> [https://www.reddit.com/r/mintmobile/comments/n96hml/when\\_will\\_mint\\_mobile\\_have\\_2fa/](https://www.reddit.com/r/mintmobile/comments/n96hml/when_will_mint_mobile_have_2fa/).

of its accountholders to implement a security passcode on their MINT accounts -- the lack of which makes the porting process even easier and even more prone to fraud:.



47. As noted in Mr. Kassim’s public posting, the “*broader set of security items*” were not in place in early-June 2021.

48. In essence, the only information that an unauthorized person would need to take over a MINT subscriber’s account and have the subscriber’s phone service ported to a different carrier is: (1) the victim’s 10-digit telephone number, (2) the victim’s MINT account number, (3) the 5-digit ZIP Code of the victim’s registered service address, and (4) [if implemented on an account] some sort of “PIN verification.”

49. Using the above-criteria and/or other personal identifying information provided by MINT about a MINT accountholder (in this case, through MINT’s systemwide data leak), the thief impersonates the actual MINT accountholder and instructs a different mobile telecommunications provider (*e.g.*, AT&T, Verizon, or T-Mobile) to initiate a computerized “port request” with MINT to have the accountholder’s phone number transferred away from MINT and to the new service provider.

50. Although the “port request” is commonly categorized as a computer-to-computer interaction, the request must be initiated by the new mobile telecommunications provider by inputting the necessary validating criteria and identifying information -- something that can only take place if the requesting party knows that validating criteria and identifying information.

51. In the case of an unauthorized SIM port, that information is illegally obtained from and/or illegally provided by MINT.

52. By getting the target’s MINT wireless telephone number transferred to a new SIM card that he owns, the thief is able to **bypass all security measures** in place on the accountholder’s account to effectuate the transfer.

53. Whether acting as a co-conspirator to the theft or through willful and/or abject negligence, MINT transfers (or “ports”) to the unauthorized person the MINT accountholder’s wireless telephone number -- disconnecting the telephone number from the actual MINT accountholder’s wireless phone’s SIM card and then connecting the telephone number to a SIM card under the control of the unauthorized person.

54. From there, the victim loses MINT service (including the ability to send or receive talk, text, or data transmissions), given that only one SIM card can be connected to MINT’s network with any given telephone number at a time.

55. Using the information provided by MINT, the thief then assumes the victim’s electronic identity, beginning with his electronic mail address, which the thief overtakes employing a simple “Password Reset” feature that requires control of the victim’s cellphone number (which was supplied to the thief by MINT).

56. Having been delivered the victim’s MINT telephone number and, directly or indirectly, his electronic mail address, the thief then diverts to himself access to the victim’s banking and investment accounts (including cryptocurrency holdings) by similarly using the victim’s MINT telephone number as a “recovery method” to reset passwords and access to those accounts -- even if the victim had two-factor authentication activated as a security measure on his accounts.

57. At that point, the thief absconds with the victim’s cryptocurrency holdings and other personal assets -- all triggered by MINT enabling the unauthorized person the ability to bypass the security measures MINT represented to its accountholder would keep his personal information safe from theft.

58. To be clear, simply *knowing* an accountholder’s cellphone number or e-mail address is not enough. The key is having **control** over and securing those vital electronic gateways to information and communication; and MINT has contumaciously placed the keys to those gates directly into the unauthorized person’s hands while simultaneously denying its accountholders their power over such things.

**PLAINTIFF'S SIM PORT AND HACK AND THEFT OF PLAINTIFF'S ASSETS**

59. On June 8, 2021, Plaintiff communicated with MINT Customer Service representatives and, for security purposes, implemented on his MINT account the "PIN Verification" feature, which required that a one-time temporary passcode be timely submitted to MINT to verify that any change being requested on his MINT account was actually coming from Plaintiff -- the MINT accountholder, not an unauthorized interloper or hacker.

60. In the instant matter, MINT bypassed the enhanced security of which Plaintiff had availed himself just a few days earlier and provided to an unauthorized person not just all of the information the unauthorized person needed to take over Plaintiff's MINT account and get it ported but also vital additional personal identifying information that facilitated the theft of Plaintiff's identity and his cryptocurrency assets.

61. As noted above, MINT leaked some or all of the following:

**From:** Mint Mobile VIP <vip@mintmobile.com>  
**Date:** July 9, 2021 at 5:03:55 PM PDT  
**Subject:** Important message from Mint Mobile VIP Care

Between June 8, 2021 and June 10, 2021, a very small number of Mint Mobile subscribers' phone numbers, including yours, were temporarily ported to another carrier without permission. While we immediately took steps to reverse the process and restore your service, an unauthorized individual potentially gained access to some of your information, which may have included your name, address, telephone number, email address, password, bill amount, international call detail information, telephone number, account number, and subscription features.

62. Whether acting as a co-conspirator to the theft or through abject negligence, MINT transferred to the unknown and unauthorized party control over Plaintiff's mobile telephone number and e-mail address, which ultimately led to the theft of approximately Four Hundred Sixty-Six Thousand Dollars (\$466,000.00) in cryptocurrency assets from Plaintiff on or about June 11, 2021.


63. Despite Plaintiff's reasonable diligence in protecting the information required to access his e-mail and financial accounts, his efforts were thwarted when MINT handed the thief the tools needed to take control of those accounts -- namely, control over Plaintiff's cellphone number, control

over his e-mail address, and control over receipt of password-reset text messages, which is all that is needed to assume Plaintiff's digital identity as far as several of those accounts are concerned.

64. MINT ported Plaintiff's mobile phone account to another carrier (Metro by T-Mobile) on or about June 11, 2021 without Plaintiff's authorization or prior knowledge.

65. Once the unauthorized person was finally so empowered by MINT with Plaintiff's personal information, he set out to abscond with Plaintiff's assets.

66. Specifically, commencing on or about June 11, 2021, the unauthorized and unknown person -- all without Plaintiff's knowledge or authorization -- withdrew from Plaintiff's cryptocurrency account the following cryptocurrency assets:

Name: Daniel Fraser			
Date: June 11, 2021, 8:08 a.m.		Mint Mobile permits unauthorized transfer of Mr. Fraser's SIM card	
Date of Cryptocurrency Theft	Cryptocurrency Assets Stolen	Location from which Assets were Stolen	Approximate Value of Funds/Assets Stolen as of Date of Theft [June 11, 2021] <sup>5</sup>
June 11, 2021 9:19 a.m.	82.446355830983653777 ETH	Ledger	\$197,909.42
June 11, 2021 9:20 a.m.	4.19851172 BTC	Ledger	\$154,232.27
June 11, 2021 9:20 a.m.	1.00066198 BTC	Ledger	\$36,759.30
June 11, 2021 9:21 a.m.	16.000609 ETH	Ledger	\$38,408.86
June 11, 2021 9:22 a.m.	0.30000449 BTC	Ledger	\$11,020.66
June 11, 2021 9:22 a.m.	0.75778501 BTC	Ledger	\$27,837.22
June 11, 2021 10:11 a.m.	0.299391 ETH	Ledger	\$716.43
TOTAL			\$466,884.16

<sup>5</sup> Valuation of the stolen funds/assets is calculated using market data compiled by [www.CoinMarketCap.com](http://www.CoinMarketCap.com), which takes the volume weighted average of all prices reported at several dozen cryptocurrency markets serving investors in the United States and abroad.

67. The theft from Plaintiff would not have occurred but for MINT's unauthorized transfer of control over Plaintiff's MINT account, MINT's failure to maintain proper security measures to prevent the unauthorized SIM port that took place, and MINT's denial of service to Plaintiff during the critical timeframe in which Plaintiff was unable to monitor the unauthorized person's efforts to steal Plaintiff's assets by using, *inter alia*, Plaintiff's own cellphone number.

**MINT'S STATUTORY OBLIGATION TO PROTECT CUSTOMERS' PERSONAL INFORMATION**

68. As a common carrier, MINT is obligated to protect the confidential personal information of its customers under Section 222 of the FCA [47 U.S.C. § 222].

69. Section 222(a) [47 U.S.C. § 222(a)] provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of and relating to ... customers ...." The "confidential proprietary information" referred to in Section 222(a) is abbreviated herein as "CPI."

70. Section 222(c) [47 U.S.C. § 222(c)] additionally provides that:

[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

The "customer proprietary network information" referred to in Section 222(c) is abbreviated herein as "CPNI."

71. Section 222(h)(1) [47 U.S.C. § 222(h)(1)] defines CPNI as: "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier, except that term does not include subscriber list information."

72. The FCC has promulgated rules to implement Section 222 "to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI." *See*, 47 CFR § 64.2001 *et seq.* ("CPNI Rules"); CPNI Order, 13 FCC Rcd. at

1 8195 ¶ 193. The CPNI Rules limit disclosure and use of CPNI without customer approval to certain  
 2 limited circumstances (such as cooperation with law enforcement), none of which are applicable to the  
 3 facts here. 47 CFR § 64.2005.

4 73. The CPNI Rules require carriers to implement safeguards to protect customers' CPNI.  
 5 These safeguards include: (i) training personnel "as to when they are and are not authorized to use  
 6 CPNI"; (ii) establishing "a supervisory review process regarding carrier compliance with the rules";  
 7 and (iii) filing annual compliance certificates with the FCC. 47 CFR § 64.2009(b), (d), and (e).

8 74. The CPNI Rules further require carriers to implement measures to prevent the disclosure  
 9 of CPNI to unauthorized individuals. 47 CFR § 64.2010. For example, "carriers must take reasonable  
 10 measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 CFR §  
 11 64.2010(a). Moreover, "carriers must properly authenticate a customer prior to disclosing CPNI based  
 12 on customer-initiated telephone contact, online account access, or an in-store visit." *Id.* In the case of  
 13 in-store access to CPNI, "[a] telecommunications carrier may disclose CPNI to a customer who, at a  
 14 carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID  
 15 matching the customer's account information." 47 CFR § 64.2010(d) (emphasis added). "Valid photo  
 16 ID" is defined in 47 CFR § 64.2003(r) as "a government-issued means of personal identification with  
 17 a photograph such as a driver's license, passport, or comparable ID that is not expired."

18 75. More than a decade ago, the FCC was already aware that there was "a substantial need  
 19 to limit the sharing of CPNI with others" because the "black market for CPNI has grown exponentially  
 20 with an increased market value placed on obtaining this data, and there is concrete evidence that the  
 21 dissemination of this private information does inflict specific and significant harm on individuals,  
 22 including harassment and the use of the data to assume a customer's identity." *See, In the Matter of*  
 23 *Implementation of the Telecommunications Acts of 1996: Telecommunications Carriers' Use of*  
 24 *Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd. 6927  
 25 (2007) ("**Pretexting Order**"), at Pg. 22 ¶39.

26 76. The FCC refers to obtaining CPNI from customers through common social engineering  
 27 ploys as "pretexting." Pretexting is "the practice of pretending to be a particular customer or other  
 28 authorized person in order to obtain access to that customer's call detail or other private

communications records.” *Id.*, at 6927 n. 1. Such “call detail” and “private communications” are CPI and CPNI under the FCA. *Id.* at 6928 *et seq.* The FCC concluded that “pretexters have been successful at gaining unauthorized access to CPNI” and that “carriers’ record on protecting CPNI demonstrate[d] that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI.” *Id.* at 6933.

77. Within this context, the FCC modified its rules to impose additional security for carriers’ disclosure of CPNI and to require that law enforcement and customers be notified of security breaches involving CPNI. *Id.* at 6936-62.

78. In its Pretexting Order, the FCC stated that it “fully expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.” *Id.* at 6959, ¶64. The FCC further stated that “[w]e decline to immunize carriers from possible sanction for disclosing customers’ private information without appropriate authorization.” *Id.* at 6960, ¶66.

79. In a statement directly relevant to the facts alleged below, **the FCC also stressed the fact that someone having obtained information fraudulently is strong evidence of the carrier’s failure to satisfy the requirements of section 222.** The FCC stated that “we hereby put carriers on notice that the Commission henceforth will infer from evidence that a pretexter has obtained unauthorized access to a customer’s CPNI that the carrier did not sufficiently protect that customer’s CPNI. A carrier then must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier’s policies and procedures, are reasonable in light of the threat posed by pretexting and the sensitivity of the customer information at issue.” *Id.* at 6959, ¶ 63 (emphasis added).

80. As further alleged below, MINT violated Section 222 of the FCA and the CPNI Rules and ignored the warning in the Pretexting Order on or before June 11, 2021, when its employees provided hackers with Plaintiff’s SIM card containing or allowing access to Plaintiff’s personal information, including CPI and CPNI, without Plaintiff’s authorization or permission and without requiring that the individual accessing Plaintiff’s account comply with MINTs own procedures.

**MINT'S OWN TERMS AND CONDITIONS AND PRIVACY POLICY ACKNOWLEDGE**  
**MINT'S OBLIGATIONS TO ITS CUSTOMERS' PRIVACY AND SECURITY**

81. In its **Terms & Conditions**<sup>6</sup> and its Privacy Statement ("**Privacy Policy**")<sup>7</sup>, including its Customer Proprietary Network Information Policy ("**CPNI Policy**"), MINT acknowledges its responsibilities to protect customers' "Personal Information" under the FCA, the CPNI Rules, and other regulations.

82. In its Privacy Policy and Terms and Conditions, MINT makes binding promises and commitments to Plaintiff, as its customer, that it will protect and secure his "Personal Information." The Privacy Policy defines "Personal Information" as "*information that identifies or is associated with a specific individual, such as a name, address, email address, or telephone number*" and also includes the following among the information that it collects from and about its customers: "*your name, billing address(es), phone number, port-in phone number, email address, and credit card number.*"

83. MINT also collects information relating to the use of its networks, products and services. "Personal Information" thus includes both CPI and CPNI under Section 222 of the FCA and the CPNI Rules.

84. In its Terms and Conditions, MINT states that it: "*use[s] technology and security features and strict policy guidelines to safeguard the privacy of CPNI and protect it from unauthorized access or improper use.*"

85. Similarly, in its Terms and Conditions, under its CPNI Policy, MINT states that it: "*does not disclose CPNI outside of Mint Mobile, its affiliates and their respective agents without customer consent except as required by law.*"

86. As alleged herein, MINT flagrantly violated its commitments to Plaintiff in its Privacy Policy and Terms and Conditions, as well as its legal obligations under the FCA, the CPNI Rules, and other laws, by turning over to hackers Plaintiff's wireless number that allowed hackers to access his "Personal Information," including CPNI.

<sup>6</sup> See <https://www.mintmobile.com/plan-terms-and-conditions/>, a true and correct copy of which is attached hereto as **Exhibit "B"**.

<sup>7</sup> See <https://www.mintmobile.com/privacy-policy/>, a true and correct copy of which is attached hereto as **Exhibit "C"**.

**MINT FAILED TO FULFILL ITS STATUTORY, COMMON LAW, AND SELF-ACKNOWLEDGED DUTIES --  
EXPOSING PLAINTIFF TO A SIM PORT AND THEFT OF \$466,000.00 OF HIS ASSETS**

87. By its procedures, practices, and regulations, MINT engages in practices that, taken together, fail to provide reasonable and appropriate security to prevent unauthorized access to its customer wireless accounts, allowing unauthorized persons to be authenticated and then granted access to sensitive customer wireless account data.

88. In particular, MINT has failed to establish or implement reasonable policies, procedures, or regulations governing MINT for the creation and authentication of user credentials for authorized customers accessing MINT accounts, creating unreasonable risk of unauthorized access. As such, at all times material hereto, MINT has failed to ensure that only authorized persons have such access and that customer accounts are secure.

89. Among other things, MINT:

- (a) fails to establish or enforce rules sufficient to ensure only authorized persons have access to MINT customer accounts;
- (b) fails to adequately safeguard and protect its customer wireless accounts, including that of Plaintiff, so wrongdoers were able to obtain access to his account;
- (c) permits the sharing of and access to user credentials among MINT's agents or employees without a pending request from the customer, thus reducing likely detection of, and accountability for, unauthorized accesses;
- (d) allows porting out of phone numbers without properly confirming that the request is coming from the legitimate customers;
- (e) lacks proper monitoring solutions and thus fails to monitor its systems for the presence of unauthorized access in a manner that would enable MINT to detect the intrusion so that the breach of security and diversion of customer information was able to occur in Plaintiff's situation and continue until after his virtual currency account was compromised;
- (f) fails to implement simple, low-cost, and readily-available defenses to identity thieves such as delaying transfers from accounts to allow for additional verifications from the customers; and
- (g) fails to build adequate internal tools to help protect its customers against hackers and account takeovers, including compromise through phone porting and wrongdoing by its own agents or employees acting on their own behalf or on behalf or at the request of a third party.

1           90. By the security practices and procedures described here, MINT established user  
2 credential structures that created an unreasonable risk of unauthorized access to customer accounts,  
3 including that of Plaintiff.

4           91. Upon information and belief, MINT has long been aware about the security risks  
5 presented by, *inter alia*, its weak user credential structures or procedures. From prior attacks on  
6 customer accounts, MINT has long had notice of those risks. For example, the FCC published its  
7 Pretexting Order in 2007, the FTC's Chief Technologist published "Your mobile phone account could  
8 be hijacked by an identity thief" in June 2016, *Forbes* published an article about SIM swapping in  
9 December 2016, and the *New York Times* published "Identity Thieves Hijack Cellphone Accounts to  
10 Go After Virtual Currency" in August 2017. Nevertheless, MINT still does not use readily-available  
11 security measures such as unique, customer-selected account passcodes to prevent or limit such  
12 foreseeable attacks.

13           92. As a result of MINT's faulty security practices, an attacker could easily gain access to a  
14 customer's account and then use it to gain access to the customer's sensitive information such as bank  
15 accounts or virtual currency accounts, among other things.

16           93. As such, MINT's security measures were entirely inadequate to protect its customers,  
17 including Plaintiff.

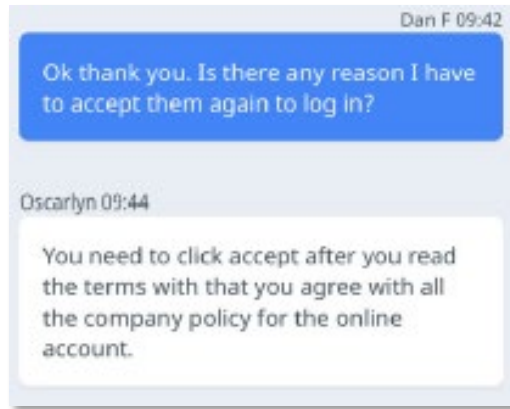
18           94. Lack of adequate security in MINT's systems, practices, or procedures enabled the  
19 wrongdoers to access Plaintiff's wireless account, which then enabled the wrongdoers to access his  
20 virtual currency account and possibly other sensitive information.

21           95. As such, MINT failed in the responsibility it owed to Plaintiff to protect his account and  
22 his phone number. Even if the subject incident were due to an "inside" job or human performance  
23 falling short, MINT is responsible for its agents. And, while MINT can automate certain customer  
24 service functions, MINT cannot transfer accountability.

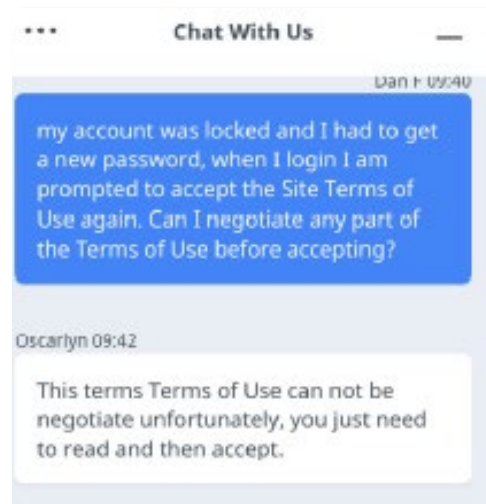
25           96. Had MINT provided adequate account security or exercised reasonable oversight,  
26 Plaintiff would not have lost his phone number or otherwise been damaged.

27           97. As a result of the foregoing acts, errors, and omissions by MINT, Plaintiff has been  
28 damaged in an amount that will be proven at the trial in this matter.





104. Further, to even login to Plaintiff's account, he was told he "*need[ed] to click accept after you agree with all the company policy for the online account.*"



105. Attached hereto as **Exhibit "D"** is a true and correct copy of Plaintiff's chat session with MINT.

106. MINT has virtually unlimited power over its customers, including Plaintiff, as seen below by the fact that it purports to hold Plaintiff and all other wireless users to the terms of an agreement that they may well have never seen or read.

107. The version of the Agreement posted on April 19, 2021 purports to govern MINT's provision of wireless service to all customers, including Plaintiff.

108. The Agreement contains numerous unconscionable terms that renders it unenforceable in its entirety because its central purpose is tainted with illegality.

109. The Agreement states that it includes not only the MINT T&C but also “*our website Terms of Use,*” any subscriber agreement or transaction materials you sign or accept, “*the service plan(s) that you choose as set forth in our written services and transaction materials that we provide or refer you to during the sales transaction (if your service plan is not specifically set forth in any printed materials, the requirements and terms set forth in the current written services and transaction materials apply, excluding plan charges and number of minutes included in your service plan),*” any confirmation materials provided by MINT, any terms set forth in any applicable coverage map brochures, and “*any other supplemental terms and conditions that we provide or otherwise make available to you.*” The Agreement further obliquely references the applicability of MINT’s Privacy Policy, Acceptable Use Policy, and Mobile Application End User License.

110. Through such language, MINT apparently contends that not only the Agreement, but all other agreements and terms referenced therein, bind all wireless customers, whether or not such customers have seen the Agreement or are aware of its terms. In other words, every time (and at any time) MINT produces a new and more onerous version of its agreements, its unsuspecting customers are purportedly bound by the new terms. This practice highlights the fact that not only are these contracts not negotiable, they are invisible. What you don’t see, you still get.

111. Furthermore, the Agreement states that if MINT does “*limit, suspend or terminate your Service and later reinstate your Service, you may be charged a reinstatement fee.*” MINT not only has unlimited power to limit or suspend a subscriber’s Service without notice; if for any reason MINT unilaterally decides to suspend and later reinstate the subscriber’s Service, the subscriber will be charged a fee.

112. The Agreement is a classic contract of adhesion imposed by MINT upon a party with no bargaining power. In contrast, MINT has unchecked power to insist upon its own terms even if the consumer is unaware of the terms of the Agreement itself. There is no ability to negotiate any term of the Agreement. It is literally “take it or leave it.”

113. The Agreement is void as against public policy as a contract of adhesion purporting to bind customers who have never heard or seen the agreement and most likely are entirely unaware of its provisions.

114. The Agreement is void and unenforceable in its entirety because it also contains exculpatory provisions, damage waivers, and an indemnification provision that purport to prevent consumers from bringing any claims against MINT obtaining redress for their claims -- even for intentional acts or gross negligence by MINT.

115. The exculpatory provision in the Agreement (“Exculpatory Provision”) contains numerous provisions that are contrary to public policy because they attempt to exempt MINT from responsibility for its own gross negligence, fraud, and violations of law. In pertinent part, the Exculpatory Provision states that:

**DISCLAIMER OF WARRANTIES:** Except to the extent otherwise expressly provided in writing, and to the extent permitted by law, the mint mobile services and devices are provided on an “as is,” “as available” and “with all faults” basis and without warranties of any kind. We make no representations or warranties, express or implied, including any implied warranty of merchantability, non infringement of the rights of third parties, or fitness for a particular purpose concerning your service or your device. We do not promise uninterrupted or error-free service and we do not authorize anyone to make any representations or warranties on our behalf. We do not guarantee that your communications will be private or secure.

\* \* \*

**LIMITATION OF LIABILITY:** Unless prohibited by law, our liability for damages or other monetary relief for any claims you may have against us is strictly limited to no more than the amounts actually paid by you to us for the service from which the damages or other liability arose in the three (3) months immediately preceding the event giving rise to the claim. You expressly agree that under no circumstances are we liable for any indirect, special, consequential, treble, exemplary or punitive damages arising out of our service (including the provision of or failure to provide same), any device, or otherwise in connection with this agreement or the subject matter hereof, regardless of the form of action and whether or not we have been informed of, or otherwise might have anticipated, the possibility of such damages.

(emphasis in original).

116. The Exculpatory Provision renders the entire Agreement unenforceable on public policy grounds because it purports to exempt MINT from its gross negligence, statutory violations, and willful behavior, including the egregious conduct “with all faults” alleged herein.

1           117. The Exculpatory Provision is further against public policy because it purports to exempt  
2 MINT from violation of statutory obligations, including the obligation to maintain the confidentiality  
3 and security of its customers' private and personal information under Section 222 of the FCA.

4           118. Moreover, the Exculpatory Provision is invalid because it allocates all the risks to the  
5 consumer with MINT disclaiming numerous forms of damages for its own conduct -- even for fraud,  
6 gross negligence, and statutory violations, including those governed by the FCA.

7           119. Thus, even if MINT deliberately handed over a customer's CPNI to hackers in violation  
8 of Section 222 of the FCA, a customer would not be entitled to the full range of damages afforded by  
9 that statute under the Exculpatory Provision.

10           120. The Exculpatory Provision is contained in a lengthy form contract drafted by a  
11 domineering telecommunication provider with vast assets in a far superior bargaining position to the  
12 wireless user. Indeed, as Plaintiff himself experienced when he tried to negotiate MINT's T&Cs, it is  
13 no exaggeration to say that the consumer has no bargaining power as regards MINT -- particularly as  
14 to the Exculpatory Provision and other draconian provisions in the Agreement. Because the  
15 Exculpatory Provision is found in a document posted on a website that, by fiat, is automatically made  
16 applicable to customers, customers may not even be aware that they have virtually no redress against  
17 MINT, unless they diligently monitor changes in the website.

18           121. Moreover, the Exculpatory Provision is contained in a complex and lengthy contract  
19 that provides essential wireless services -- without which most customers have no means of  
20 communication (including for emergency services), let alone essential computing, geolocation, texting,  
21 research or other services.

22           122. The Exculpatory Provision -- included in a contract of adhesion as to which MINT's  
23 users, including Plaintiff, have no bargaining authority -- is void because it is plainly unconscionable  
24 and against public policy.

25           123. The Exculpatory Provision is also substantively unconscionable because it allocates  
26 risks in an objectively unreasonable manner.

124. The allocation of risks under the Agreement is objectively unreasonable because MINT takes upon itself virtually no liability and purports to exempt itself from virtually all damages, including those arising out of its own deliberate, grossly negligent, or fraudulent acts.

125. The Agreement is further unenforceable because customers are purportedly required to indemnify MINT for all claims arising out of the services provided by MINT, including claims that arise due to MINT's negligence, gross negligence, deliberate conduct, or statutory violations.

126. The indemnity provision in the Agreement ("Indemnification") states:

**You agree to defend, indemnify, and hold us harmless from and against any and all losses, claims, liabilities, costs and expenses (including taxes, fees, fines, penalties, interest, expenses of investigation and attorneys' fees and disbursements) as incurred, arising out of or relating to use of the Mint Mobile Service or Devices, breach of the Agreement, or violation of any laws or regulations or the rights of any third party by you or any person on your account or that you allow to use your Mint Mobile Service or Device.**

(emphasis added).

127. Read literally, the Indemnification requires a consumer, such as Plaintiff, to hold MINT harmless for MINT's own negligence, deliberate behavior, gross negligence, statutory violations (including disclosure of CPNI under the FCA), or fraud for any conduct arising out of "*use of the Service*" or even MINT's "*breach of the Agreement*."

128. On its face, the indemnity provision in a contract of adhesion renders the entire Agreement unconscionable and unenforceable because it defeats the entire purpose of the contract by making it impossible for consumers to bring claims against MINT for the entire range of statutory rights to which a consumer, such as Plaintiff, is entitled.

129. Indeed, the Indemnification would totally obviate MINT's commitment to privacy in its Privacy Policy as well as its legal obligations under the FCA and the CPNI Rules.

130. Because the entire Agreement is unenforceable because the central purpose of the Agreement is tainted with illegality so that the contract as a whole cannot be enforced, the arbitration provision in the Agreement ("Arbitration Provision") is also unenforceable.

131. The Arbitration Provision would require Plaintiff to arbitrate his claims without affording the full range of statutory remedies, including indirect, special, consequential, treble, or

punitive damages that are available to him under the claims alleged herein. For example, Plaintiff, if required to arbitrate this claim, would be forced by the Exculpatory Provision to forego his statutory entitlement to punitive damages for MINT's fraud and negligence.

132. Moreover, the Arbitration Provision would require Plaintiff to forego the full range of damages to which he is entitled under his claim for relief under the Federal Communications Act § 222.

133. These defects render not only the Arbitration Provision, but also the entire Agreement, unenforceable.

134. Because the defenses raised by Plaintiff as to the unconscionability of the Agreement are "enforced evenhandedly" and do not "interfere[ ] with the fundamental attributes of arbitration," they do not run afoul of *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2010). The Court's decision in *Concepcion* did not abrogate the savings clause of the FAA that provides that arbitration agreements may be declared unenforceable "upon such grounds as exist at law or in equity for the revocation of any contract," including "generally applicable contract defenses, such as fraud, duress, or unconscionability." *Concepcion* at 339, quoting 9 U.S.C. § 2 and *Doctors Associates, Inc. v. Casarotto*, 517 U.S. 681, 687 (1996). For the reasons alleged in this claim, such defenses apply squarely to the Agreement.

135. There is an actionable and justiciable controversy between Plaintiff and MINT in that Plaintiff contends that the Agreement, including the Exculpatory Provision, Indemnification, and Arbitration Provision, is unenforceable in its entirety because it is unconscionable and void against public policy since it prevents consumers, such as Plaintiff, from obtaining redress against MINT even for deliberate acts in violation of its legal duties.

136. A declaration of the (un)enforceability of the Agreement, including the Exculpatory Provision, Indemnification, and Arbitration Provision and all other provisions of the Agreement, is necessary and appropriate.

WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment against Defendant MINT MOBILE, a Delaware limited liability company, declaring that the Agreement in its entirety is unenforceable as unconscionable and against public; or, in the alternative that: (a) the Exculpatory Provision is unenforceable as against Plaintiff; (b) the Indemnification is

unenforceable as against Plaintiff; and (c) the Arbitration Provision is unenforceable as against Plaintiff. Plaintiff further requests entry of any and all other relief the Court deems just and proper.

**COUNT II – BREACH OF FEDERAL COMMUNICATIONS ACT [47 U.S.C. §§ 206, 222]**  
**(UNAUTHORIZED DISCLOSURE OF CUSTOMER CONFIDENTIAL PROPRIETARY**  
**INFORMATION AND PROPRIETARY NETWORK INFORMATION)**

Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1 through 100 above, as if they were fully set forth herein, and further alleges:

137. MINT is a “common carrier” engaging in interstate commerce by wire regulated by the Federal Communications Act (“FCA”) and subject to the requirements, *inter alia*, of sections 206 and 222 of the FCA.

138. Under section 206 of the FCA [47 U.S.C. § 206], “[i]n case any common carriers shall do, or cause or permit it to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney’s fee, to be fixed by the court in every case of recovery, which attorney’s fee shall be taxed and collected as part of the costs in the case.”

139. Section 222(a) of the FCA [47 U.S.C. § 222(a)] requires every telecommunications carrier to protect, among other things, the confidentiality of proprietary information of, and relating to, customers (“CPI”).

140. Section 222(c)(1) of the FCA [47 U.S.C. § 222(c)(1)] further requires that, “[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to customer proprietary network information [‘CPNI’] in its provision of (A) telecommunications services from which such information is derived, or (B) services necessary to or used in the provision of such telecommunication services . . . .”

141. The information disclosed to hackers by MINT in the June 2021 SIM port fraud transferring Plaintiff’s telephone number was CPI and CPNI under Section 222 of the FCA.

142. MINT failed to protect the confidentiality of Plaintiff's CPI and CPNI, including his wireless telephone number, account information, and his private communications, by divulging that information to hackers.

143. Through its negligence, gross negligence and deliberate acts, including inexplicable failures to follow its own security procedures, supervise its employees, the CPNI Regulations, the warnings of the Pretexting Order, its Privacy Policy, and CPNI Policy, and by allowing its employees to bypass such procedures, MINT permitted hackers to access Plaintiff's telephone number, telephone calls, text messages and account information to steal approximately \$466,000.00 worth of his cryptocurrency.

144. As a direct consequence of MINT's violations of the FCA, Plaintiff has been damaged by loss of approximately \$466,000.00 worth in cryptocurrency, which MINT allowed to fall into the hands of thieves, and for other damages in an amount to be proven at the Final Hearing in this matter.

145. Plaintiff is also entitled to his attorney's fees under the FCA in bringing this action against MINT for its gross negligence and fraudulent misrepresentation as to the security that it provides for customer accounts as required by the FCA and the CPNI Regulation.

WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment against Defendant MINT MOBILE, a Delaware limited liability company; for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Court deems just and proper.

**COUNT III – VIOLATION OF 18 U.S.C. § 1030(a)(2)(C) and 1030(a)(4)**  
**(COMPUTER FRAUD AND ABUSE ACT [“CFAA”])**

Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1 through 100 above, as if they were fully set forth herein, and further alleges:

146. This cause of action asserts a claim against MINT for violations of 18 U.S.C. § 1030(a)(2)(C) and 1030(a)(4) (the “Computer Fraud and Abuse Act”) for aiding and abetting authorized access to a protected computer to obtain information, for knowingly doing so with an intent to defraud, and for furthering fraudulent activity thereby to obtain something of value.

147. Plaintiff's cellphone is a "protected computer" as defined in 18 U.S.C. § 1030(e)(2)(B) because it is used in interstate or foreign commerce or communication, including sending and receiving electronic mail, sending and receiving text messages, and accessing and interacting with the internet.

148. MINT aided and abetted an unauthorized and unknown person by granting to that person, acting knowingly and with intent to defraud Plaintiff, access to a protected computer (*i.e.*, Plaintiff's cellphone).

149. MINT divulged to an unauthorized person Plaintiff's personal identifying information and transferred to that unauthorized person Plaintiff's cellphone number and the telecommunications services tied thereto through Plaintiff's cellphone.

150. MINT aided and abetted the unauthorized transfer of Plaintiff's SIM card despite the clear barrier of security protocols on Plaintiff's account that MINT overtly ignored and bypassed -- a barrier that MINT expressly represented to Plaintiff was put in place to prevent an unauthorized SIM port.

151. As a consequence of MINT's actions and omissions, Plaintiff has suffered damage far in excess of Five Thousand Dollars (\$5,000.00).

152. Moreover, as a consequence of MINT interrupting Plaintiff's service, he has suffered damage far in excess of Five Thousand Dollars (\$5,000.00).

WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment against Defendants MINT MOBILE, a Delaware limited liability company, for damages, including compensatory damages, punitive damages, interest, expenses, and any other relief the Court deems just and proper.

**COUNT IV – VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW -**  
**CAL. BUS. & PROF. CODE § 17200 et seq.**  
**(UNLAWFUL BUSINESS PRACTICE)**

Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1 through 100 above, as if they were fully set forth herein, and further alleges:

153. This cause of action asserts a claim against MINT for engaging in unlawful business practices within the meaning of California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200 *et seq.*

154. The conduct set forth herein is a “business practice” within the meaning of the UCL.

155. MINT stored and processed Plaintiff’s Personal Information, including CPI and CPNI, in its electronic systems and databases. Plaintiff’s CPNI and other Personal Information could readily be accessed when Plaintiff’s telephone number was transferred out to new telephones controlled by hackers. All such information is “Personal Information” under MINT’s Privacy Policy.

156. MINT falsely represented to Plaintiff and other customers in its T&C and its Privacy Policy that: (a) its system was secure and that it would respect the privacy of its customers’ information; (b) it had established electronic and administrative safeguards designed to make the information it collects from its customers secure; and (c) it *“uses technology and security features and strict policy guidelines to safeguard the privacy of CPNI and protect it from unauthorized access or improper use.”* These security measures and safeguards included those mandated by the CPNI Rules.

157. MINT knew or should have known that it did not employ reasonable, industry-standard, and appropriate security measures that complied with “legal requirements,” in the FCA, CPNI Rules, and other laws and regulations.

158. Plaintiff was entitled to assume that MINT would take appropriate measures to keep secure his Personal Information, including CPI and CPNI, because of MINT’s statements in its T&C and its Privacy Policy.

159. MINT did not disclose at any time that Plaintiff’s CPI and CPNI were vulnerable to hackers because MINT’s security measures were ineffective.

160. MINT, which was the only party possessing material information as to its own practices, did not disclose the rampant defects in its security procedures, when it had a duty to make such a disclosure.

161. MINT further violated the UCL by: (a) failing to implement reasonable and appropriate security measures for Plaintiff’s Personal Information, as required by the FCA, the CPNI Rules, and California law, or following industry standards for data security, and (b) failing to comply with MINT’s own T&C and Privacy Policy.

162. If MINT had complied with those legal requirements, Plaintiff would not have suffered the damages related to the June 11, 2021 SIM port fraud.

163. Moreover, Plaintiff would not have lost his MINT service (for which he paid MINT) during the critical timeframe in which Plaintiff was unable to monitor the unauthorized person's efforts to steal Plaintiff's assets by using, *inter alia*, Plaintiff's own cellphone number.

164. MINT's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, the FCA, 47 U.S.C. §§ 206 and 222, the CPNI Rules, Cal. Civ. Code § 1798.81.5(b), Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), Cal. Bus. & Prof. Code § 22576 (because MINT failed to comply with MINT's own posted privacy policies), and the Consumer Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.*

165. Plaintiff suffered injury-in-fact and loss money or property, including stolen cryptocurrencies worth nearly \$466,000.00, as a result of MINT's unlawful business practices.

166. Plaintiff has lost the benefit of his bargain for his purchased services from MINT that he would not have paid had he known the truth regarding MINT's inadequate data security.

167. Because of MINT's unlawful business practices and violation of the UCL, Plaintiff is entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment against Defendant MINT MOBILE, a Delaware limited liability company; for equitable relief and damages, including compensatory damages, punitive damages, interest, attorneys' fees, expenses, and any other relief the Court deems just and proper.

**COUNT V – VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW -**  
**CAL. BUS. & PROF. CODE § 17200 *et seq.***  
**(UNLAWFUL BUSINESS PRACTICE)**

Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1 through 100 above, as if they were fully set forth herein, and further alleges:

168. This cause of action asserts a claim against MINT for engaging in unlawful business practices within the meaning of California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200 *et seq.*

169. MINT stored and processed Plaintiff's Personal Information, including CPI and CPNI, in its electronic system and databases.

1 170. Plaintiff's Personal Information was readily accessed when hackers, through SIM port  
2 fraud, gained access to Plaintiff's telephone number.

3 171. MINT represented to Plaintiff through its T&C and its Privacy Policy that its systems  
4 and databases were secure and that his Personal Information would remain private and secure and  
5 would not be divulged to unauthorized third parties.

6 172. MINT engaged in unfair acts and business practices by representing in its Privacy Policy  
7 that it had established electronic and administrative safeguards designed to make the information MINT  
8 collected from and about Plaintiff secure.

9 173. MINT further represented that its employees followed the COBC and that such  
10 employees "*do[ ] not disclose CPNI outside of Mint Mobile, its affiliates and their respective agents*  
11 *without customer consent except as required by law.*"

12 174. Even without those misrepresentations, Plaintiff was entitled to, and did, assume MINT  
13 would take appropriate measures to keep his Personal Information safe under the FCA, the CPNI Rules,  
14 and other laws and regulations.

15 175. MINT did not disclose at any time that Plaintiff's Personal Information was vulnerable  
16 to hackers as a result of MINT employees turning over that Personal Information, including and  
17 allowing access to his telephone number.

18 176. MINT also did not disclose that its security measures were inadequate and outdated, its  
19 employees were not properly trained, or that its security procedures could readily be bypassed in  
20 commission of activity harmful to accountholders.

21 177. MINT knew or should have known it did not employ reasonable security and that it  
22 lacked adequate employee training and monitoring measures that would have kept Plaintiff's personal  
23 and financial information secure and prevented the loss or misuse of Plaintiff's Personal Information.

24 178. MINT violated the UCL by misrepresenting, both by affirmative conduct and by  
25 omission, the security of its systems and services, and its ability to safeguard Plaintiff's Personal  
26 Information, including CPI and CPNI.

179. MINT also violated the UCL by failing to implement and maintain reasonable security procedures and practices appropriate to protect Plaintiff's Personal Information under the FCA and CPNI Rules, including CPI and CPNI.

180. If MINT had followed the industry standards and legal requirements, Plaintiff would not have suffered the damages related to the June 11, 2021 SIM port fraud.

181. In addition, Plaintiff would not have lost his MINT service (for which he paid MINT) during the critical timeframe in which Plaintiff was unable to monitor the unauthorized person's efforts to steal Plaintiff's assets by using, *inter alia*, Plaintiff's own cellphone number.

182. MINT also violated its commitment to maintain the confidentiality and security of Plaintiff's Personal Information, including CPI and CPNI, and failed to comply with its own policies and applicable laws, regulations, including the FCA, CPNI Rules, and industry standards relating to data security.

183. The harm caused by MINT's actions and omissions, as described in detail in this pleading, greatly outweighs any perceived utility. Indeed, MINT's failure to follow data security protocols, its own policies, and its misrepresentations to Plaintiff had no utility at all.

184. MINT's actions and omissions, as described above, violated fundamental public policies expressed by the United States and California. *See, e.g.*, FCA, 47 U.S.C. § 222; CPNI Rules; Cal. Civ. Code § 1798.1 ("The [California] Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); and Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.).

185. MINT's acts and omission, and the injuries caused by MINT, are thus comparable to or the same as a violation of law.

186. The harm caused by MINT's actions and omissions, as described in detail above, is substantial in that it has caused Plaintiff to suffer approximately \$466,000.00 in actual financial harm because of MINT's unfair business practices.

187. Because of MINT's unfair business practices and violations of the UCL, Plaintiff is entitled to restitution, disgorgement of wrongfully obtained profits, and injunctive relief.

WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment against Defendant MINT MOBILE, a Delaware limited liability company; for equitable relief and damages, including compensatory damages, punitive damages, interest, attorneys' fees, expenses, and any other relief the Court deems just and proper.

**COUNT VI – VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW -**  
**CAL. BUS. & PROF. CODE § 17200 et seq.**  
**(UNLAWFUL BUSINESS PRACTICE)**

Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1 through 100 above, as if they were fully set forth herein, and further alleges:

188. This cause of action asserts a claim against MINT for engaging in unlawful business practices within the meaning of California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200 et seq.

189. MINT affirmatively represented to Plaintiff that his Personal Information, including CPI and CPNI, was secure and that it would remain private.

190. MINT engaged in fraudulent acts and business practices by misleadingly misrepresenting in its Privacy Policy that it "*uses technology and security features and strict policy guidelines to safeguard the privacy of CPNI and protect it from unauthorized access or improper use.*"

191. MINT not only made affirmative misrepresentations, but also made fraudulent omissions by concealing true facts from Plaintiff.

192. MINT did not disclose to Plaintiff that its data security measures were woefully substandard, that its employees could bypass its security measures, and that it did not adequately supervise or monitor its employees so that they would adhere to the commitments it made in the Privacy Policy, as well as the requirements of the FCA and CPNI Rules.

193. MINT's representations that it would secure Plaintiff's Personal Information were facts that reasonable persons could be expected to rely upon when deciding whether to use (or continue to use) MINT's services.

194. Plaintiff suffered injury and lost money when MINT transferred his wireless telephone number to a hacker's phone that allowed the hacker to steal approximately \$466,000.00 worth of cryptocurrency during the critical timeframe in which Plaintiff was unable to monitor the unauthorized person's efforts to steal Plaintiff's assets by using, *inter alia*, Plaintiff's own cellphone number.

195. Because of MINT's fraudulent business practices and violations of the UCL, Plaintiff is entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief.

WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment against Defendant MINT MOBILE, a Delaware limited liability company; for equitable relief and damages, including compensatory damages, punitive damages, interest, attorneys' fees, expenses, and any other relief the Court deems just and proper.

#### COUNT VII – NEGLIGENCE

Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1 through 100 above, as if they were fully set forth herein, and further alleges:

196. MINT owed a duty to Plaintiff to exercise reasonable care in safeguarding and protecting his Personal Information, including CPI and CPNI, and keeping it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties.

197. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's Personal Information, including CPI and CPNI, was adequately secured and protected.

198. MINT knew that Plaintiff's Personal Information, including CPI and CPNI, was confidential and sensitive.

199. Indeed, MINT acknowledged this in its Privacy Policy.

200. MINT likewise knew that Plaintiff's Personal Information was vulnerable to hacks by thieves and other criminals both because it acknowledged such in its Privacy Policy.

1           201. MINT thus knew of the substantial and foreseeable harms that could occur to Plaintiff  
2 if it did not place adequate security on his Personal Information and did not follow its own security  
3 measures for the account.

4           202. By being entrusted by Plaintiff to safeguard his Personal Information, including CPI and  
5 CPNI, MINT had a special relationship with Plaintiff.

6           203. Plaintiff signed up for MINT's wireless services and agreed to provide his Personal  
7 Information to MINT with the understanding that MINT would take appropriate measures to protect it.  
8 But MINT did not protect Plaintiff's Personal Information and violated his trust.

9           204. MINT breached its duty to exercise reasonable care in safeguarding and protecting  
10 Plaintiff's Personal Information, including CPI and CPNI, by failing to adopt, implement, and maintain  
11 adequate security measures to safeguard that information, including its duty under the FCA, the CPNI  
12 Rules, and its own Privacy Policy.

13           205. MINT's failure to comply with federal and state requirements for security further  
14 evidences MINT's negligence in failing to exercise reasonable care in safeguarding and protecting  
15 Plaintiff's Personal Information, including CPI and CPNI.

16           206. But for MINT's wrongful and negligent breach of its duties owed to Plaintiff, his  
17 Personal Information, including his CPI and CPNI, would not have been compromised, stolen, viewed,  
18 and used by unauthorized persons.

19           207. MINT's negligence was a direct and legal cause of the theft of Plaintiff's Personal  
20 Information and the legal cause of his resulting damages, including, but not limited to, the theft of  
21 approximately \$466,000.00 worth of cryptocurrency.

22           208. The injury and harm suffered by Plaintiff was the reasonably foreseeable result of  
23 MINT's failure to exercise reasonable care in safeguarding and protecting Plaintiff's Personal  
24 Information, including his CPI and CPNI.

25           209. MINT's misconduct as alleged herein is malice, fraud, or oppression in that it was  
26 despicable conduct carried on by MINT with a willful and conscious disregard of the rights or safety  
27 of Plaintiff and despicable conduct that has subjected Plaintiff to cruel and unjust hardship in conscious  
28 disregard of his rights.

1           210. As a result, Plaintiff is entitled to punitive damages against MINT.

2           WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment  
3 against Defendant MINT MOBILE, a Delaware limited liability company; for equitable relief and  
4 damages, including compensatory damages, punitive damages, interest, attorneys' fees, expenses, and  
5 any other relief the Court deems just and proper.

6                           **COUNT VIII – NEGLIGENT MISREPRESENTATION**

7           Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1  
8 through 100 above, as if they were fully set forth herein, and further alleges:

9           211. MINT made numerous representations and false promises in its Privacy Policy  
10 regarding the supposed security of consumers' Personal Information, including Plaintiff's Personal  
11 Information.

12           212. Such representations and promises were false because MINT was using outdated and  
13 inadequate security procedures and failed to disclose that it did not adhere to its own standards,  
14 including the security standards that it purportedly implemented for Plaintiff in or prior to June 11,  
15 2021 or the CPNI Rules.

16           213. MINT's misrepresentations and false promises, including those made in or prior to June  
17 2021, were material to Plaintiff, who reasonably relied upon those representations and promises.

18           214. Plaintiff would not have agreed to continue to use and pay for MINT's services if he  
19 had known that they were not as secure as represented by MINT and would not have lost approximately  
20 \$466,000.00.

21           215. MINT intended that Plaintiff rely on its representations and promises, as it knew that  
22 Plaintiff would not entrust his Personal Information to unreasonable security risks.

23           216. In reliance upon MINT's representations and promises, Plaintiff continued to maintain  
24 a wireless account with MINT and to use his MINT phone number for verification and other purposes.

25           217. As a direct and proximate result of MINT's wrongful actions, Plaintiff has been  
26 damaged by paying monthly fees to MINT and having thieves steal approximately \$466,000.00 worth  
27 of cryptocurrency through the SIM port fraud on June 11, 2021.

28           WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment

1 against Defendant MINT MOBILE, a Delaware limited liability company; for equitable relief and  
 2 damages, including compensatory damages, punitive damages, interest, attorneys' fees, expenses, and  
 3 any other relief the Court deems just and proper.

4 **COUNT IX – NEGLIGENT TRAINING AND SUPERVISION**

5 Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1  
 6 through 100 above, as if they were fully set forth herein, and further alleges:

7 218. MINT owed Plaintiff a duty to exercise reasonable care in supervising and training its  
 8 MINT employees to safeguard and protect Plaintiff's Personal Information, including CPI and CPNI,  
 9 and to keep it from being compromised, lost, stolen, misused and/or disclosed to unauthorized parties.

10 219. MINT knew that Plaintiff's Personal Information, including CPI and CPNI, was  
 11 confidential and sensitive.

12 220. By being entrusted by Plaintiff to safeguard his Personal Information, including CPI and  
 13 CPNI, MINT had a special relationship with Plaintiff.

14 221. Plaintiff signed up for MINT's wireless services and agreed to provide his Personal  
 15 Information to MINT with the understanding that MINT's employees would take appropriate measures  
 16 to protect it.

17 222. MINT also made promises in the Privacy Policy and CPNI Policy that its employees  
 18 would respect its customers' privacy and that MINT would supervise and train its employees to adhere  
 19 to its legal obligations to protect their Personal Information.

20 223. MINT breached its duty to supervise and train its employees to safeguard and protect  
 21 Plaintiff's Personal Information, including CPI and CPNI, by not requiring them to adhere to its  
 22 obligations under the CPNI Rules and other legal provisions.

23 224. MINT is morally culpable, given prior security breaches involving its own employees.

24 225. MINT breached its duty to exercise reasonable care in supervising and monitoring its  
 25 employees to protect Plaintiff's Personal Information, including CPI and CPNI.

26 226. MINT's failure to comply with the requirements of the FCA and CPNI Rules further  
 27 evidence MINT's negligence in adequately supervising and monitoring its employees so that they  
 28 would safeguard and protect Plaintiff's Personal Information, including CPI and CPNI.

227. But for MINT's wrongful and negligent breach of its duties to supervise and monitor its employees, Plaintiff's CPI and CPNI would not have been disclosed to unauthorized individuals through SIM port fraud.

228. MINT's negligence was a direct and legal cause of the theft of Plaintiff's Personal Information and the legal cause of his resulting damages, including, but not limited to, the theft of approximately \$466,000.00 worth of cryptocurrency.

229. The injury and harm suffered by Plaintiff was the reasonably foreseeable result of MINT's failure to supervise and monitor its employees in safeguarding and protecting Plaintiff's Personal Information, including his CPI and CPNI.

230. MINT's misconduct as alleged here was done with malice, fraud and oppression in that it was despicable conduct carried on by MINT with a willful and conscious disregard of the rights or safety of Plaintiff and despicable conduct that has subjected Plaintiff to cruel and unjust hardship in conscious disregard of his rights. As a result, Plaintiff is entitled to punitive damages against MINT.

WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment against Defendant MINT MOBILE, a Delaware limited liability company; for equitable relief and damages, including compensatory damages, punitive damages, interest, attorneys' fees, expenses, and any other relief the Court deems just and proper.

#### **COUNT X – BREACH OF CONTRACT**

Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1 through 100 above, as if they were fully set forth herein, and further alleges:

231. The Privacy Policy and Terms and Conditions coalesce to form a binding contract between MINT and Plaintiff.

232. MINT breached the contract with respect to at least the following provisions of the Privacy Policy and Terms and Conditions:

(a) MINT *“uses technology and security features and strict policy guidelines to safeguard the privacy of CPNI and protect it from unauthorized access or improper use.”*

(b) MINT *“does not disclose CPNI outside of Mint Mobile, its affiliates and their respective agents without customer consent except as required by law.”*

1 (c) MINT “take[s] precautions and have implemented certain technical measures  
 2 intended to protect against unauthorized access to, disclosure of, and unlawful  
 3 interception of personal information submitted via this Site, including Secure  
 4 Sockets Layer (“SSL”) for all financial transactions through this Site.”

5 (d) MINT assures its accountholders: “Mint Mobile has a duty, to protect the  
 6 confidentiality of information regarding your telephone use, the services you  
 7 purchase from us, the calls you place and the location of your device on our  
 8 network when you make a telephone call.”

9 233. MINT also breached its Privacy Policy and Terms and Condition by failing to follow  
 10 not only the letter of the law, but the spirit of the law by failing to protect Plaintiff’s privacy.

11 234. MINT breached these provisions of its Privacy Policy and CPNI Policy in its Terms and  
 12 Conditions by not having proper safeguards in accordance with law, including the FCA and the CPNI  
 13 Rules, to protect Plaintiff’s “Personal Information,” including CPI and CPNI.

14 235. MINT further breached its promises by not limiting access to Plaintiff’s Personal  
 15 Information to authorized or properly-trained individuals.

16 236. MINT likewise violated its commitments to maintain the confidentiality and security of  
 17 Plaintiff’s Personal Information by failing to comply with its own policies and applicable law, rules,  
 18 regulations, court and/or administrative orders that apply to MINT’s business -- including, specifically,  
 19 the legal requirements and company policies surrounding the privacy of communications and the  
 20 security and privacy of MINT customer records.

21 237. MINT thus breached its obligations under the FCA and the CPNI Rules.

22 238. The SIM port fraud that occurred on June 11, 2021 was a direct and legal cause of the  
 23 injuries and damages suffered by Plaintiff, including loss of approximately \$466,000.00 of  
 24 cryptocurrency.

25 239. To the extent that MINT maintains that the Exculpatory Provision, Damages Restriction,  
 26 and the Indemnification in the Agreement apply to the promises made by MINT in the Privacy Policy  
 27 and Terms and Conditions, such provisions, as well as the Agreement in its entirety, are unenforceable  
 28 and do not apply to the Privacy Policy and Terms and Conditions.

1           240. Moreover, such provisions are unconscionable because an entity cannot exculpate itself  
2 from its obligations to maintain the privacy and security of personal information under federal and state  
3 law.

4           241. Plaintiff was harmed due to MINT's breach of the terms of the Privacy Policy and Terms  
5 and Conditions Agreement, because his "Personal Information," including CPI and CPNI, was breached  
6 in the June 11, 2021 SIM port fraud, which led to monetary losses of approximately \$466,000.00.

7           WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment  
8 against Defendant MINT MOBILE, a Delaware limited liability company; for equitable relief and  
9 damages, including compensatory damages, punitive damages, interest, attorneys' fees, expenses, and  
10 any other relief the Court deems just and proper.

11                           **COUNT XI – BREACH OF IMPLIED CONTRACT**

12           Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1  
13 through 100 above, as if they were fully set forth herein, and further alleges:

14           242. To the extent that MINT's Privacy Policy and Terms and Conditions did not form  
15 express contracts, the opening of an MINT wireless account by Plaintiff created implied contracts  
16 between MINT and Plaintiff as to the protection of his Personal Information, the terms of which were  
17 set forth by the relevant Privacy Policy and Terms and Conditions.

18           243. MINT breached such implied contracts by failing to adhere to the terms of the applicable  
19 Privacy Policy and Terms and Conditions.

20           244. Specifically, MINT violated its commitment to maintain the confidentiality and security  
21 of the Personal Information of Plaintiff, including CPI and CPNI, and failed to comply with its own  
22 policies and applicable law, rules, regulations, court and/or administrative orders that apply to MINT's  
23 business -- including, specifically, the legal requirements and company policies surrounding the privacy  
24 of communications and the security and privacy of MINT customer records.

25           245. Plaintiff was harmed because of MINT's breach of the terms of the Privacy Policy, and  
26 Terms and Conditions because his "Personal Information," including CPI and CPNI, were breached in  
27 the June 11, 2021 SIM port, which led to monetary losses of approximately \$466,000.00.  
28

1 WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment  
 2 against Defendant MINT MOBILE, a Delaware limited liability company; for equitable relief and  
 3 damages, including compensatory damages, punitive damages, interest, attorneys' fees, expenses, and  
 4 any other relief the Court deems just and proper.

5 **COUNT XII – BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING**

6 Plaintiff realleges and incorporates by reference each and every allegation in paragraphs 1  
 7 through 100 above, as if they were fully set forth herein, and further alleges:

8 246. There is an implied covenant of good faith and fair dealing in every contract that neither  
 9 party will do anything which will injure the right of the other to receive the benefits of the agreement.

10 247. Under the express and implied terms of the relationship between Plaintiff and MINT,  
 11 including through the Privacy Policy and Terms and Conditions, Plaintiff was to benefit using MINT's  
 12 services, while MINT was supposed to benefit through money received for Plaintiff subscribing to  
 13 MINT's wireless services.

14 248. MINT exhibited bad faith through its conscious awareness of and deliberate indifference  
 15 to the risk to Plaintiff's Personal Information, including CPI and CPNI, by: (a) not implementing  
 16 security measures adequate to protect his Personal Information; (b) improperly hiring, training, and  
 17 supervising its employees; (c) not adhering to its own security standards; and (d) failing to invest in  
 18 adequate security protections.

19 249. MINT, by exposing Plaintiff to vastly greater security risks, breached its implied  
 20 covenant of good faith and fair dealing with respect to the terms of its Privacy Policy and Terms and  
 21 Conditions and the implied warranties of its contractual relationship with its users.

22 250. Plaintiff was harmed because of MINT's breach of the implied covenant of good faith  
 23 and fair dealing because his Personal Information was compromised by the hackers in the in the SIM  
 24 port of June 11, 2021, which led to monetary damages of approximately \$466,000.00.

25 251. MINT's misconduct as alleged herein is fraud in that it was deceit or concealment of a  
 26 material fact known to MINT conducted with an intent on the part of MINT of depriving Plaintiff of  
 27 legal rights or otherwise concerning injury.  
 28

252. In addition, MINT's misconduct, as alleged herein, is malice, fraud or oppression in that it was despicable conduct carried on by MINT with a willful and conscious disregard of the rights or safety of Plaintiff and has subjected Plaintiff to cruel and unjust hardship in conscious disregard of his rights. As a result, Plaintiff is entitled to punitive damages against MINT.

WHEREFORE, Plaintiff DANIEL FRASER, an individual, demands entry of a judgment against Defendant MINT MOBILE, a Delaware limited liability company; for equitable relief and damages, including compensatory damages, punitive damages, interest, attorneys' fees, expenses, and any other relief the Court deems just and proper.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff DANIEL FRASER, an individual, respectfully prays for relief as follows:

- (a) A declaration that Defendant MINT MOBILE's Agreement in its entirety is unenforceable as unconscionable and against public; or, in the alternative that: (a) the Exculpatory Provision is unenforceable as against Plaintiff; (b) the Indemnification is unenforceable as against Plaintiff; and (c) the Arbitration Provision is unenforceable as against Plaintiff;
- (b) A judgment awarding Plaintiff equitable restitution, including, without limitation, restoration of the status quo ante, and return to Plaintiff all cryptocurrency or fiat currency taken from him in connection with the SIM card port negligently-allowed by Defendant MINT;
- (c) An award of any and all additional damages recoverable under law including but not limited to compensatory damages, punitive damages, incidental damages, and consequential damages;
- (d) Pre- and post-judgment interest;
- (e) Attorneys' fees, expenses, and the costs of this action; and
- (f) All other and further relief as the Court deems necessary, just, and proper.

### **DEMAND FOR JURY TRIAL**

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff demands trial by jury in this action of all issues so triable.

**RESERVATION OF RIGHTS**

Plaintiff reserves his right to further amend this Complaint, upon further investigation and discovery, to assert any additional claims for relief against Defendant or other parties as may be warranted under the circumstances and as allowed by law.

Respectfully submitted,

By: /s/ Matt Putterman  
Matt Putterman (CA Bar No. 306845)  
**PUTTERMAN LAW, APC**  
23 Corporate Plaza Drive - Suite 150  
Newport Beach, CA 92660  
Telephone: (949) 271-6382  
E-Mail: [Matt@Putterman-Law.com](mailto:Matt@Putterman-Law.com)

David C. Silver, Esq. (*pro hac vice* forthcoming)  
**SILVER MILLER**  
11780 W. Sample Road  
Coral Springs, Florida 33065  
Telephone: (954) 516-6000  
E-Mail: [DSilver@SilverMillerLaw.com](mailto:DSilver@SilverMillerLaw.com)

*Attorneys for Plaintiff Daniel Fraser*

Dated: January 7, 2022